PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	10/759,241
Confirmation Number:	7209
Filing Date:	January 16, 2004
Applicants:	Kristy L. BIRT, James P. GODDARD and Kerry L. LAUREN
Title:	METHOD, APPARATUS AND PROGRAM STORAGE DEVICE FOR PROVIDING AUTOMATED TRACKING OF SECURITY VULNERABILITIES
Examiner:	Devin E. ALMEIDA
Group Art Unit:	2132
Attorney Docket No.:	END920030052US1 (1397-9U)

Mail Stop Appeal Brief - Patents
Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed October 10, 2008, and in response to the Final Office Action dated September 10, 2008, wherein Appellant appeals from the Examiner's rejection of Claims 1, 5-6, 8-12, 16-17, 19-23 and 25-30.

TABLE OF CONTENTS

I. Real Party in Interest

The real party in interest is International Business Machines, which is the assignee of the subject application by virtue of assignment recorded on Reel/Frame 014919/0760 on January 16, 2004.

II. Related Appeals and Interferences

None.

III. Status of Claims

Claims 1, 5-6, 8-12, 16-17, 19-23 and 25-30 are pending in this Application. Claims 2-4, 7, 13-15, 18 and 24 have been cancelled without prejudice and without disclaimer of subject matter. Claims 1, 5-6, 8-12, 16-17, 19-23 and 25-30 have been finally rejected, and it is from the final rejection of Claims 1, 5-6, 8-12, 16-17, 19-23 and 25-30 that this Appeal is taken.

IV. Status of Amendments

The claims have not been amended subsequent to the imposition of the Final Office Action dated September 10, 2008.

V. Summary of Claimed Subject Matter

The present invention, as recited in independent Claims 1, 10, 12, 21, 23 and 25-26, is directed toward methods and apparatus for providing automated tracking and a criticality factor of security vulnerabilities on a computer system, as described at least in the Summary of the Invention on pages 5-8 of the Specification.

With respect to independent Claim 1, a method for providing automated tracking of security vulnerabilities is claimed. (See FIGS. 3 and 4; page 10, lines 7-9; page 13, line 17 through page 17, line 15). The method includes using a computing device to perform a security vulnerability assessment on a system. (See FIG. 3, step 310; page 13, lines 19-20). Responsive to detecting the presence of the security vulnerability in the system, data obtained from the security vulnerability assessment is stored in a security vulnerability database. (See FIG. 3, step 390; page 14, lines 13-15). A security vulnerability score is determined using a computer program. (See FIG. 4, steps 460-40; page 15, lines 12-15; page 16, line 7 through page 17, line 4). The security vulnerability score is a product of a frequency score, a severity score, a criticality score, and a trust score. (See page 16, line 7 through page 17, line 4). The frequency score is based on a percentage of hosts experiencing the detected security vulnerability in the system. (See page 16, lines 7-11). The criticality score is based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation. (See page 16, lines 17-19). A time to fix the security vulnerability detected by the security vulnerability assessment of the system is determined based on the determined security vulnerability score. (See FIG. 4, step 460; page 15 line 12 though page 16 line 6).

Independent Claim 10 recites a method for determining a criticality factor for a security vulnerability in a computer system. (See FIGS. 3 and 4; page 14, line 20 through page 17, line 4). Security vulnerabilities detected in the computer system during a security vulnerability assessment are entered in a database. (See FIG. 3, step 390; page 14, lines 13-15). A frequency of occurrence is measured for the detected security vulnerabilities. (See FIG. 4, step 442; page 15, lines 9-11). A security vulnerability factor is assigned to a detected security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and isolation of the system. (See page 16, lines 7-22).

Independent Claim 12 recites an apparatus for providing automated tracking of security vulnerabilities. (See FIGS. 1 and 2; page 12, line 3 through page 13, line 5). The apparatus includes a memory for storing program instructions. (See FIG. 2, RAM 214, ROM 216; page 12, lines 11-13). The apparatus also includes a processor. (See FIG. 2, CPU 210; page 12, lines 10-11). The processor is configured according to the program instructions to perform a security vulnerability assessment on a system. (See FIG. 3, step 310; page 13, lines 19-20). The processor is further configured to detect the presence of a security vulnerability in the system, and responsive to detecting the presence of the security vulnerability, store data obtained from the security vulnerability assessment in a security vulnerability database. (See FIG. 3, step 390; page 14, lines 13-15). The processor is further configured to determine a security vulnerability score. (See FIG. 4, steps 460-40; page 15, lines 12-15; page 16, line 7 through page 17, line 4). The security vulnerability score is a product of a frequency score, a severity score, a criticality score, and a trust score. (See page 16, line 7 through page 17, line 4). The frequency score is based on a percentage of hosts experiencing the detected security vulnerability in the system. (See page 16, lines 7-11). The criticality score is based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation. (See page 16, lines 17-19). The processor is further configured to determine a time to fix a security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score. (See FIG. 4, step 460; page 15 line 12 though page 16, line 6).

Independent Claim 21 recites an apparatus for determining a criticality factor for a security vulnerability in a computer system. (See FIGS. 1 and 2; page 12, line 3 through page 13, line 5; page 14, line 20 through page 17, line 4). The apparatus includes a memory for storing program instructions. (See FIG. 2, RAM 214, ROM 216; page 12, lines 11-13). The apparatus also includes a processor. (See FIG. 2, CPU 210; page 12, lines 10-11). The processor is configured according to the program instructions for entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment. (See FIG. 3, step 390; page 14, lines 13-15). The processor is further configured for measuring a frequency of occurrence for the detected security vulnerabilities. (See FIG. 4, step 442; page 15, lines 9-11). The processor is further configured for assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and isolation of the system. (See page 16, lines 7-22).

Independent Claim 23 recites an apparatus for providing automated tracking of security vulnerabilities. (See FIGS. 1 and 2; page 12, line 3 through page 13, line 5). Regarding the means-plus-function clauses of Claim 23, exemplary structure in the specification for performing the claimed functions is indicated {in brackets}. General support for the claim elements in the specification is discussed separately below. The claimed apparatus includes a means {Random Access Memory (RAM) 214, Read Only Memory (ROM) 216} for storing program instructions. Claim 23 further recites a means {central processing unit 210}configured according to the program instructions provided by the means for storing for performing a security vulnerability assessment on a system, detecting the presence of a security vulnerability in the system, and responsive to detecting the presence of the security vulnerability: storing data obtained from the security vulnerability assessment in a security vulnerability database; determining a security vulnerability score, the security vulnerability score being a product of a frequency score, a severity score, a criticality score, and a trust score; and determining a time to fix a security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score.

Regarding the support for Claim 23 in the Specification, referring to FIG. 2, as described at least in pages 12-13 of the Specification, the claimed apparatus includes system 200 having a multiplicity of processing applications. (See FIGS. 1 and 2; page 12, line 3 through page 13, line 5). The claim recites a means for storing program instructions. (See FIG. 2; page 12, lines 11-13). Claim 23 further recites a means configured according to the program instructions provided by the means for storing for performing a security vulnerability assessment on a system. (See FIG. 3, step 390; page 14, lines 13-15). The means is further configured for detecting the presence of a security vulnerability in the system. (See FIG. 3, step 310; page 13, lines 19-20). Responsive to detecting the presence of the security vulnerability, the means is further configured to store data obtained from the security vulnerability assessment in a security vulnerability database. (See FIG. 3, step 390; page 14, lines 13-15). The means is further configured to determine a security vulnerability score, the security vulnerability score being a product of a frequency score, a severity score, a criticality score, and a trust score. (See page 16, line 7 through page 17, line 4). The frequency score is based on a percentage of hosts experiencing the detected security vulnerability in the system. (See page 16, lines 7-11). The criticality score is based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation. (See page 16, lines 17-19). The means is further configured to determine a time to fix a security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score. (See FIG. 4, step 460; page 15 line 12 though page 16 line 6).

Independent Claim 25 recites a program storage device readable by a computer, the program storage device tangibly embodying one or more programs of instructions executable by the computer to perform a method for providing automated tracking of security vulnerabilities. (See FIG. 2, removable data storage device 288; FIGS. 3 and 4; page 10, lines 7-9; page 13, line 17 through page 17, line 15; page 18, lines 14-22). The method includes performing a security vulnerability assessment on a system. (See FIG. 3, step 310; page 13, lines 19-20). Responsive to detecting the presence of a security vulnerability in the system, data obtained from the security vulnerability assessment is stored in a vulnerability database. (See FIG. 3, step 390; page 14, lines 13-15). A security vulnerability score is determined based on a frequency score, a severity score, a criticality score, and a trust score. (See page 16, line 7 through page 17, line 4). The frequency score is based on a percentage of hosts experiencing the detected security vulnerability in the system. (See page 16, lines 7-11). The criticality score is based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation. (See page 16, lines 17-19). A time to fix a security vulnerability detected by the security vulnerability assessment of the system is determined based on the determined security vulnerability score. (See FIG. 4, step 460; page 15 line 12 though page 16 line 6).

Independent Claim 26 recites a program storage device readable by a computer, the program storage device tangibly embodying one or more programs of instructions executable by the computer to perform a method for determining a criticality factor for a security vulnerability in a computer system. (See FIG. 2, removable data storage device 288; FIGS. 3 and 4; page 10, lines 7-9; page 13, line 17 through page 17, line 15; page 18, lines 14-22). The method includes entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment. (See FIG. 3, step 390; page 14, lines 13-15). A frequency of occurrence for the detected security vulnerabilities is measured. (See FIG. 4, step 442; page 15, lines 9-11). A security vulnerability factor is assigned to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and isolation of the system. (See page 16, lines 7-22).

VI. Grounds of Rejection to be Reviewed on Appeal

1. Claims 1, 4-9, 12, 15-20, 23, 25 and 27-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent No. 7,243,148, issued to Keir *et al.* (hereinafter "Keir") in view of United States Patent No. 5,944,825, issued to Bellemore *et al.* (hereinafter "Bellemore").
2. Claims 10, 11, 21, 22 and 26 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Keir, in view of Bellemore, and further in view of United States Patent Publication No. 2004/0006704, to Dahlstrom *et al.* (hereinafter "Dahlstrom").

VII. Argument

A. <u>The Rejection of Claims 1, 4-9, 27 and 28 under 35 U.S.C. § 103(a)</u>

Claims 1, 4-9, 27 and 28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Keir in view of Bellemore. Applicant disagrees with this conclusion as the Examiner has failed to cite a reference or combination of references disclosing or suggesting each and every element of Applicant's Claimed Invention, as required to establish a *prima facie* case of obviousness.

When determining the patentability of a claimed invention, the Examiner initially bears the burden of establishing a *prima facie* conclusion of obviousness. MANUAL OF PATENT EXAMINING PROCEDURE (MPEP), § 2142. The Federal Circuit has stated that "rejections on obviousness cannot be sustained with mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988; 78 U.S.P.Q.D.2d (BNA) 1329, 1351 (Fed. Cir. 2006). See also *KSR International Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741; 82 U.S.P.Q.2d (BNA) 1385 (2007)(quoting Federal Circuit statement with approval).

A conclusion that a claim would have been obvious is supported when "all the claimed elements were known in the prior art and one skilled in the art could have combined the elements as claimed by known methods with no change in their respective functions, and the combination yielded nothing more than predictable results to one of ordinary skill in the art." MPEP § 2143(A) (citing *KSR*, 127 S. Ct. at 1739).

Independent Claim 1

Regarding Claim 1, the Examiner incorrectly contends that Keir teaches "determining, using a computer program, a security vulnerability score, the security vulnerability score being a ***product*** of a frequency score, a severity score, a criticality score, and a trust score, the frequency score based on a percentage of hosts experiencing ***the detected security vulnerability*** in the system and the criticality score based on whether ***at least one of confidential data and personal data is on the system*** and whether ***information on the element is used for aggregation***," (emphasis added). Applicant disagrees with this assessment.

Specifically, on page 2 of the Office Action, in response to Applicants' arguments, the Examiner explicitly states that Keir teaches F (the security vulnerability score) is computed by:

$$F = 100 - V - E$$

where

$$V = \min(70, (70V_h H_h + 42V_m H_m + 14V_l H_l)/H_n)$$

and

$$E = \min\left(30, \sum_{y=1 \to H_n} \{R_y + W_y + 30T_y\}\right).$$

In the above equations, the Examiner identifies the "security vulnerability" as "F," and the "frequency score" as being "calculated in the V part of the security vulnerability score where $H_h H_m H_l$ make up the number of host (*sic*) that have high, medium, and low vulnerabilities on them." The Examiner further identifies the "severity score" as being "calculated in the V part of the security vulnerability score where high vulnerability are multiplied by 70 (root access) medium by 42 and low by 14," and the "criticality score" as "E." Finally, the Examiner equates the "trust score" as "the nodes that don't have a high medium or low vulnerability of the total nodes of the network H_n."

Even assuming for a moment that the Examiner's identifications are valid, it is abundantly clear that Keir does ***not*** teach that the security vulnerability score is the ***product*** of "a frequency score, a severity score, a criticality score, and a trust score," as recited in Claim 1. As can readily be seen above, the Examiner's reasoning equates the security vulnerability score to the ***difference*** between 100 and the ***sum*** of a ***function*** of a frequency score and a severity score and a criticality score, wherein the criticality score is a function of a trust score. Thus, the

Examiner's contention that Keir teaches the security vulnerability score being the ***product*** of "a frequency score, a severity score, a criticality score, and a trust score," is simply without merit.

A product, in mathematical terms, is defined as "the result obtained by multiplying two or more quantities together."[1] It is well-known that "patent claims must be given their 'accustomed', 'ordinary', or dictionary meaning unless the available interpretation aids point to another meaning."[2] "If there is a discernable plain and ordinary meaning of the claim language, then this meaning usually defines the scope of the claims unless the patentee has explicitly disclaimed or clearly avowed this meaning in the specification or prosecution history," *Housey Pharmaceuticals, Inc. v. Astrazeneca UK Ltd.*, 366 F.3d 1348, 1352; 70 U.S.P.Q.2d (BNA) 1641 (Fed. Cir. 2004). Thus, the Examiner's assessment of the function $F = 100 - V - E$ disclosed by Keir as a ***product*** of "a frequency score, a severity score, a criticality score, and a trust score" is incorrect.

Moreover, on page 17, lines 1-2 of the Specification of the present invention, Applicants clearly define the security vulnerability score as simply a final score determined by the equation, Final Score = Frequency Score * Severity Score * Criticality Score * Trust Score.

Additionally, Keir does not teach the element of Claim 1 where the frequency score is "based on a percentage of hosts experiencing ***the detected security vulnerability*** in the system." The Examiner equates the "frequency score" as being "calculated in the V part of the security vulnerability score where $H_h H_m H_l$ make up the number of host (*sic*) that have high, medium, and low vulnerabilities on them." The security vulnerability score of Claim 1 is directed specifically toward a assessing a score for the "***detected security vulnerability.***" In contrast, the

[1] Dictionary.com, "product," in *Dictionary.com Unabridged (v 1.1)*. Source location: Random House, Inc. http://dictionary.reference.com/browse/product. Available: http://dictionary.reference.com. Accessed: November 14, 2008.

[2] 5A DONALD S. CHISUM, CHISUM ON PATENTS § 18.03[2][b] (2007).

function *F* disclosed in Keir is a "FoundScore" which determines an "internal network vulnerability indicia" that indicates the vulnerability of ***an entire network***. (See Keir, column 63, lines 4-26). Thus, none of the terms H_h, H_m, or H_l are indicative of the percentage of hosts experiencing the ***detected security vulnerability*** on the system. Instead, each term is all-inclusive of the number of hosts on the system that have low, medium or high level vulnerabilities. Thus, each term most likely includes more hosts than actually experience the ***detected security vulnerability***, but there is no way to discern the actual number from this term.

Also, Claim 1 recites that the criticality score is "based on whether ***at least one of confidential data and personal data is on the system*** and whether ***information on the element is used for aggregation***." The Examiner equates the criticality score to the term "E," which Keir denotes as an "Exposure Loss." (See Keir, column 64, line 26). According to Keir, the Exposure Loss is a function of the sum of all rogue applications, wireless access points, and Trojan horses or backdoors on all hosts of the network. (See Keir, column 65, lines 5-24). Thus, Keir's Exposure Loss is a function of the number and types of vulnerabilities found throughout the system, with no focus at all on the ***characteristics of a particular host*** where a specific security vulnerability is found. In contrast, the claimed element requires that the criticality score is "based on ***at least one of confidential data and personal data is on the system*** and whether ***information on the element is used for aggregation***." Keir is silent regarding these criteria.

Additionally, Bellemore does not teach the above-described claimed features, nor does the Examiner represent such. Both Keir and Bellemore, whether considered standing alone or in combination, fail to teach, disclose or suggest each and every element as recited in Claim 1, as required to establish a *prima facie* case of obviousness. Accordingly, the Examiner's rejection with respect to Claim 1 should be reversed.

Dependent Claims 4-9, 27 and 28

Although the Office Action states that Claims 4 and 7 are rejected under 35 U.S.C. § 103(a) as unpatentable over Keir in view of Bellemore, Applicants have previously cancelled these claims, rendering the rejection moot. Dependent Claims 5-6, 8-9, 27 and 28 depend directly or indirectly from independent Claim 1 and are believed patentable at least by virtue of their dependency.

B. The Rejection of Claims 12, 16-20, 23, 25, 29 and 30 under 35 U.S.C. § 103(a)

Claims 12, 16-20, 23, 25, 29 and 30 are also rejected under 35 U.S.C. § 103(a) as being unpatentable over Keir in view of Bellemore. Applicants do not agree.

Independent Claims 12, 23 and 25

Independent Claims 12, 23 and 25 also recite features similar to those discussed above in relation to Claim 1. Specifically, independent Claim 12 includes "an apparatus for providing automated tracking of security vulnerabilities" which includes "a processor, configured according to the program instructions for … determining a security vulnerability score, the security vulnerability score being a ***product*** of a frequency score, a severity score, a criticality score, and a trust score; the frequency score based on a percentage of hosts experiencing ***the detected security vulnerability*** in the system; and the criticality score based on whether ***at least one of confidential data and personal data is on the system*** and whether ***information on the element is used for aggregation***" (emphasis added). Independent Claim 23 recites "an apparatus for providing automated tracking of security vulnerabilities" including "means configured according to the program instructions provided by the means for storing for … determining a security vulnerability score, the security vulnerability score being a ***product*** of a frequency score, a severity score, a criticality score, and a trust score; the frequency score based on a percentage of hosts experiencing ***the detected security vulnerability*** in the system; and the criticality score based on whether ***at least one of confidential data and personal data is on the system*** and whether ***information on the element is used for aggregation***" (emphasis added). Independent Claim 25 recites "a program storage device readable by a computer" containing "programs of instructions executable by the computer to perform a method for providing automated tracking of security vulnerabilities," including "determining a security vulnerability score based on a frequency score, a severity score, a criticality score, and a trust score; the frequency score based on a percentage of hosts experiencing ***the detected security vulnerability in the system***; and the criticality score based on whether ***at least one of confidential data and personal data is on the system*** and whether ***information on the element is used for aggregation***" (emphasis added). Thus, the arguments presented above in relation to Claim 1, apply equally to independent Claims 12, 23 and 25 and the rejections under 35 U.S.C. § 103(a) should be reversed.

Dependent Claims 15-20, 29 and 30

Although the Office Action states that Claims 15 and 18 are rejected under 35 U.S.C. § 103(a) as unpatentable over Keir in view of Bellemore, Applicants have previously cancelled these claims, rendering the rejection moot. Dependent Claims 16, 17, 19, 20, 29 and 30 depend directly or indirectly from independent Claim 12 and are believed patentable at least by virtue of their dependency.

C. The Rejection of Claims 10 and 11 under 35 U.S.C. § 103(a)

Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Keir in view of Bellemore, and in further view of Dahlstrom. Though the Examiner declares that these claims are rejected in view of the combination of Keir, Bellemore and Dahlstrom, no specific element of any claim is credited as being taught by Bellemore. Having reviewed Bellemore and determined that the features recited in the above claims are not taught, disclosed or suggested by Bellemore, Applicants are hereby treating the rejection as encompassing the combination of Keir and Dahlstrom.

Independent Claim 10

Regarding Claim 10, the Examiner incorrectly contends that Keir discloses "a method for determining a criticality factor for a security vulnerability in a computer system," and "assigning a security vulnerability factor to a detected security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and ***isolation*** of the system." Applicants disagree with this contention.

Additionally, "statements in the preamble reciting the purpose or intended use of the claimed invention must be evaluated to determine whether the recited purpose or intended use results in a structural difference (or, in the case of process claims, manipulative difference) between the claimed invention and the prior art. If so, the recitation serves to limit the claim." MANUAL OF PATENT EXAMINING PROCEDURES § 2111.02 (8th ed. September 2007).

The preamble of Claim 10 recites "a method for determining a criticality factor for ***a security vulnerability*** in a computer system" (emphasis added). Thus, the method disclosed in Claim 10 relates to a single security vulnerability. In contrast, the method taught in Keir is in reference to "a methodology for determining the security score for a ***target network***" (emphasis added)(See Keir, column 62, lines 3-4). The method disclosed in Keir considers the entire content and makeup of a complete network, including the number and types of security vulnerabilities found, whereas the method recited in Claim 10 relates to a single security vulnerability; therefore, this feature is not taught, disclosed or suggested by Keir.

As discussed above, in relation to Independent Claim 1, neither Keir nor Bellemore teach, disclose, or suggest a security vulnerability factor that is a product of a frequency score, a criticality score, a severity score, and a trust score. Independent Claim 10 is narrower in scope than Claim 1 as Claim 10 recites the actual function of the frequency score (i.e., the frequency of occurrence of the security vulnerability in the system), the criticality score (i.e., a criticality of an element in the system), the severity score (i.e., a severity of the security vulnerability within the system), and the trust score (i.e., isolation of the system), instead of classifying the functions by name. Dahlstrom also does not teach or suggest these features. Dahlstrom is directed to a process for determining a risk assessment of a security vulnerability based on the simplicity of exploiting the vulnerability, the popularity/probability of exploitation and an impact to an organization if exploited. (*See* Dahlstrom, paragraph [0062]). None of the cited references teach, disclose or suggest the recited features; therefore, Claim 10 is believed to be patentable and the Examiner's rejection should be reversed.

Additionally, the Examiner contends that Keir teaches that the security vulnerability factor is assigned to a detected security vulnerability based upon a number of factors, including "isolation of the system." Applicants disagree. Keir does not teach determining a security vulnerability factor based on the isolation of the system. Instead, the method cited by the Examiner in column 62, line 3 through column 66 line 19, relates only to "a vulnerability testing instruction set 1024 that tests ***internal*** network security and provides an objective score of ***internal*** network security," (emphasis added)(See Keir, column 63, lines 57-59). The disclosed method does not take into consideration whether or not the system is isolated when determining its "objective score of ***internal*** network security." Bellemore and Dahlston also do not teach this feature and are not cited by the Examiner as so doing. Therefore, Claim 10 is patentable and the Examiner's rejection of this claim should be reversed.

For at least the above-referenced reasons, neither Keir, Bellemore, nor Dahlstrom, whether considered standing alone or in combination, teach, disclose or suggest each and every element as recited in Claim 10, as required to establish a *prima facie* case of obviousness. Accordingly, the Examiner's rejection with respect to Claim 10 should be reversed.

Dependent Claim 11

Dependent Claim 11 depends from independent Claims 10 and is believed patentable at least by virtue of its dependency.

D. The Rejection of Claims 21, 22 and 26 under 35 U.S.C. § 103(a)

Claims 21, 22 and 26 were also rejected under 35 U.S.C. 103(a) as being unpatentable over Keir in view of Bellemore, and in further view of Dahlstrom. As discussed above with respect to Claim 10, though the Examiner declares that these claims are rejected in view of the combination of Keir, Bellemore and Dahlstrom, no specific element of any claim is credited as being taught by Bellemore. Having reviewed Bellemore and determined that the features recited in the above claims are not taught, disclosed or suggested by Bellemore, as with Claim 10, Applicants are hereby treating the rejection as encompassing the combination of Keir and Dahlstrom.

Independent Claims 21 and 26

Independent Claims 21 and 26 also recite features similar to those discussed above in relation to Claim 10. Specifically, independent Claim 21 includes "an apparatus for determining

a criticality factor for a security vulnerability in a computer system, comprising … a processor, configured according to the program instructions for … assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and ***isolation*** of the system." Likewise, independent Claim 26 recites "a program storage device readable by a computer" which includes "programs of instructions executable by the computer to perform a method for determining ***a criticality factor for a security vulnerability*** in a computer system." The method includes "assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and ***isolation*** of the system."

Thus, the arguments presented above in relation to Claim 10, apply equally to independent Claims 21 and 26 and the rejections under 35 U.S.C. § 103(a) should be reversed.

<u>Dependent Claim 22</u>

Dependent Claim 22 depends from independent Claim 12 and is believed patentable at least by virtue of its dependency.

VIII. Conclusion

For the reasons provided above as well as provided in the record, the claim rejections are believed to be improper and a result of clear error by the Examiner. Accordingly, pending Claims 1, 5-6, 8-12, 16-17, 19-23 and 25-30 are believed to be in condition for allowance, and a reversal of the Examiner's rejections is respectfully requested.

The Commissioner is hereby authorized to credit overpayments or charge payment of any additional fees associated with this communication to Deposit Account No. 090457.

Respectfully submitted,

Date: December 2, 2008 By: /Alan M. Weisberg/

Alan M. Weisberg
Reg. No.: 43,982
Attorney for Applicants
Christopher & Weisberg, P.A.
200 East Las Olas Boulevard, Suite 2040
Fort Lauderdale, Florida 33301
Customer No. 68786
Tel: (954) 828-1488
Fax: (954) 828-9122
email: ptomail@cwiplaw.com

127277

APPENDIX A: CLAIMS ON APPEAL

1. A method for providing automated tracking of security vulnerabilities, comprising:

using a computing device to perform a security vulnerability assessment on a system;

detecting the presence of a security vulnerability in the system; and

responsive to detecting the presence of the security vulnerability:

storing data obtained from the security vulnerability assessment in a security vulnerability database;

determining, using a computer program, a security vulnerability score, the security vulnerability score being a product of a frequency score, a severity score, a criticality score, and a trust score, the frequency score based on a percentage of hosts experiencing the detected security vulnerability in the system and the criticality score based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation; and

determining a time to fix the security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score.

2. (Cancelled)

3. (Cancelled)

4. (Cancelled)

5. The method of claim 1 further comprising entering an IP address associated with the security vulnerability and a description of the detected security vulnerability in a tracking database.

6. The method of claim 1 further comprising determining delinquent security vulnerabilities based upon the determined time to fix the security vulnerability detected by the security vulnerability assessment.

7. (Cancelled)

8. The method of claim 6 further comprising re-running a scan profile when notification is received that the security vulnerability has been fixed.

9. The method of claim 8 further comprising determining whether the security vulnerability still exists and archiving records associated with the security vulnerability when the security vulnerability does not still exist.

10. A method for determining a criticality factor for a security vulnerability in a computer system, comprising:

entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment;

measuring a frequency of occurrence for the detected security vulnerabilities; and

assigning a security vulnerability factor to a detected security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and isolation of the system.

11. The method of claim 10, wherein the criticality of an element in the system is based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation.

12. An apparatus for providing automated tracking of security vulnerabilities, comprising:

a memory for storing program instructions; and

a processor, configured according to the program instructions for:

performing a security vulnerability assessment on a system;

detecting the presence of a security vulnerability in the system; and

responsive to detecting the presence of the security vulnerability:

storing data obtained from the security vulnerability assessment in a security vulnerability database;

determining a security vulnerability score, the security vulnerability score being a product of a frequency score, a severity score, a criticality score, and a trust score;

the frequency score based on a percentage of hosts experiencing the detected security vulnerability in the system; and

the criticality score based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation; and

determining a time to fix a security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score.

13. (Cancelled)

14. (Cancelled)

15. (Cancelled)

16. The apparatus of claim 12, wherein the processor enters an IP address associated with the security vulnerability and a description of the detected security vulnerability in a tracking database.

17. The apparatus of claim 12, wherein the processor identifies delinquent security vulnerabilities based upon the determined time to fix the security vulnerability detected by the security vulnerability assessment.

18. (Cancelled)

19. The apparatus of claim 17, wherein the processor re-runs a scan profile when notification is received that the security vulnerability has been fixed.

20. The apparatus of claim 19, wherein the processor determines whether the security vulnerability still exists and archives records associated with the security vulnerability when the security vulnerability does not still exist.

21. An apparatus for determining a criticality factor for a security vulnerability in a computer system, comprising:

a memory for storing program instructions; and

a processor, configured according to the program instructions for entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment, measuring a frequency of occurrence for the detected security vulnerabilities and assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and isolation of the system.

22. The apparatus of claim 21, wherein the processor considers a criticality of an element in the system the criticality based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation.

23. An apparatus for providing automated tracking of security vulnerabilities, comprising:

means for storing program instructions; and

means configured according to the program instructions provided by the means for storing for:

performing a security vulnerability assessment on a system~~,~~;

detecting the presence of a security vulnerability in the system~~,~~; and

responsive to detecting the presence of the security vulnerability:

storing data obtained from the security vulnerability assessment in a security vulnerability database;

determining a security vulnerability score, the security vulnerability score being a product of a frequency score, a severity score, a criticality score, and a trust score;

the frequency score based on a percentage of hosts experiencing the detected security vulnerability in the system; and

the criticality score based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation; and

determining a time to fix a security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score.

24. (Cancelled)

25. A program storage device readable by a computer, the program storage device tangibly embodying one or more programs of instructions executable by the computer to perform a method for providing automated tracking of security vulnerabilities, the method comprising:

performing a security vulnerability assessment on a system;

detecting the presence of a security vulnerability in the system; and

responsive to detecting the presence of the security vulnerability:

storing data obtained from the security vulnerability assessment in a vulnerability database;

determining a security vulnerability score based on a frequency score, a severity score, a criticality score, and a trust score;

the frequency score based on a percentage of hosts experiencing the detected security vulnerability in the system; and

the criticality score based on whether at least one of confidential data and personal data is on the system and whether information on the element is used for aggregation; and

determining a time to fix a security vulnerability detected by the security vulnerability assessment of the system based on the determined security vulnerability score.

26. A program storage device readable by a computer, the program storage device tangibly embodying one or more programs of instructions executable by the computer to perform

a method for determining a criticality factor for a security vulnerability in a computer system, the method comprising:

entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment;

measuring a frequency of occurrence for the detected security vulnerabilities; and

assigning a security vulnerability factor to a security vulnerability based upon the frequency of occurrence of the security vulnerability in the system, a criticality of an element in the system, a severity of the security vulnerability within the system, and isolation of the system.

27. The method of claim 1, wherein the severity score is based on whether a host will allow root compromise and whether the security vulnerability is remotely exploitable.

28. The method of claim 1, wherein the trust score is based on whether the system is isolated.

29. The apparatus of claim 12, wherein the severity score is based on whether a host will allow root compromise and whether the security vulnerability is remotely exploitable.

30. The apparatus of claim 12, wherein the trust score is based on whether the system is isolated.

APPENDIX B: EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

APPENDIX C: RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.